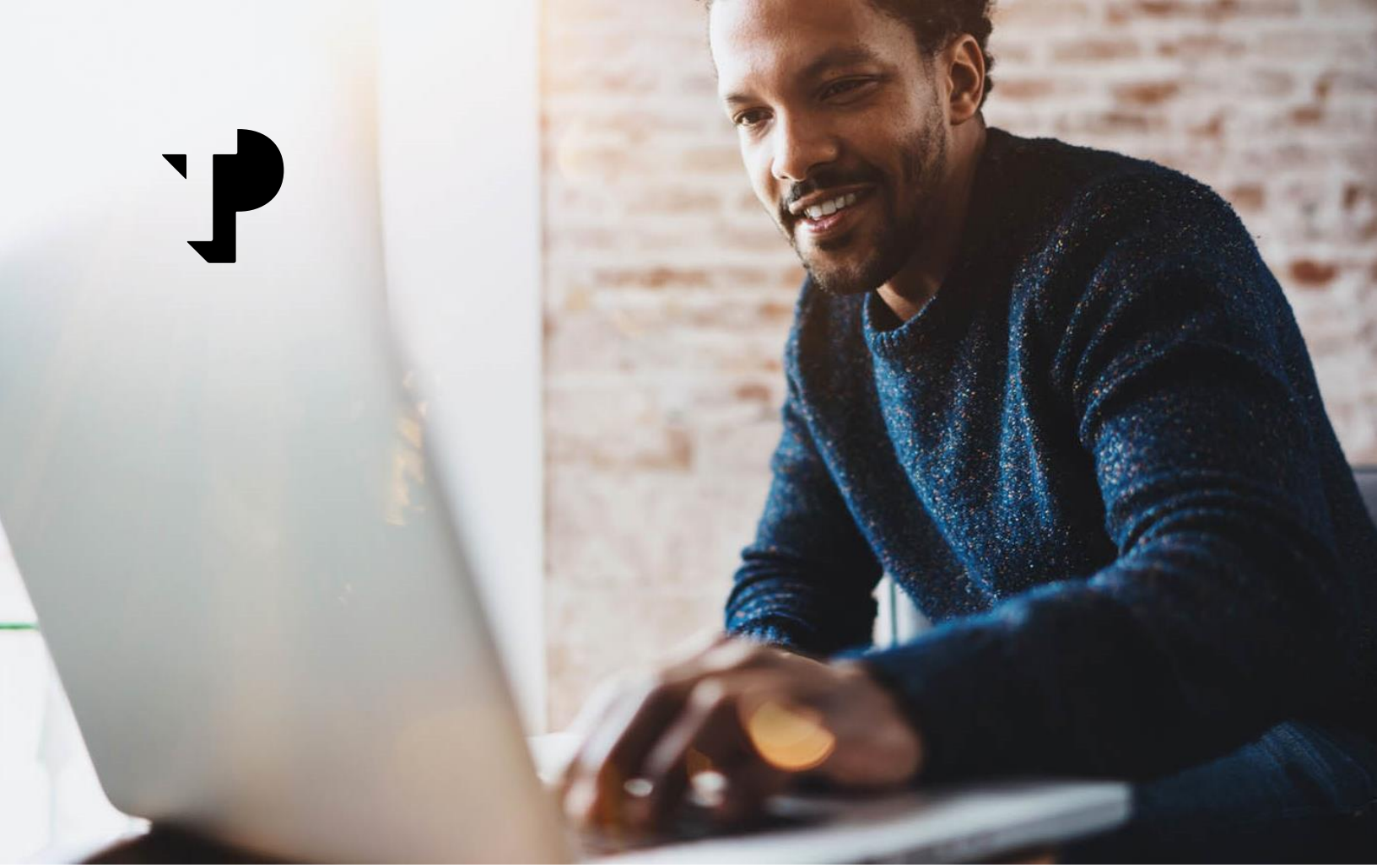

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN TP MAR

CONTENIDO

REVISION LOG

FECHA	CAMBIOS	DESCRIPCIÓN	CICLO DE APROBACIÓN
Abr/2024	No	Revisión de documento sin cambios	**Elabora:** Liliana Villar **Aprueba:** Luis Gonzalez
Ago/2024	Si	Actualización de política de acuerdo con los controles de la versión ISO 27001:2022.	**Elabora:** Liliana Villar **Aprueba:** Luis Gonzalez
Nov/2024	No	Revisión sin cambios, ajustes menores en el documento.	**Elabora:** Liliana Villar **Aprueba:** Luis González
Abr/2025	No	Actualización de logo y portada de la política.	**Elabora:** Estefania Castañeda **Aprueba:** Luis González

1. OBJETIVO

Establecer lineamientos, procedimientos y directrices que describan cómo gestiona y protege la organización sus datos sensibles y activos de información.

2. ALCANCE

Los lineamientos de la presente política son de obligatorio cumplimiento para todos los colaboradores de TP MAR, incluyendo empleados directos e indirectos, contratistas, subcontratistas y proveedores, que brinden soporte a la organización tanto desde las instalaciones físicas como desde teletrabajo.

3. RESPONSABILIDAD

- La Alta Dirección es responsable de garantizar los recursos y el apoyo necesarios para el cumplimiento de esta política.
- El Equipo del SGSI es responsable de realizar revisiones anuales del Sistema de Gestión de la Seguridad de la Información (SGSI), incluida toda la información documentada y las actividades relacionadas.
- Los proveedores de servicios, como vendedores, proveedores y contratistas, deben conocer y cumplir las políticas de la organización.
- El equipo de comunicación y relaciones públicas asegurará la comunicación y divulgación de forma física o digital dentro de la organización y accesibilidad de las partes interesadas internas y externas pertinentes.
- Los líderes de las unidades operativas son responsables de tener en cuenta esta política en todos los aspectos de sus funciones y servicios empresariales críticos.

4. AUTORIDAD

- Aprobación: Alta Dirección
- Revisión y actualización: Líder del sistema de gestión de Seguridad de la Información (ISMS).

5. DEFINICIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para administrar información confidencial con el fin de que permanezca segura. Este Implica establecer políticas, procedimientos y procesos para gestionar los riesgos y garantizar la confidencialidad, integridad y disponibilidad de los activos de la información.

6. PILARES DE LA POLÍTICA:

- Confidencialidad: Protección de datos e información sensibles frente a accesos o divulgaciones no autorizadas, tanto internas como externas.

- Integridad: Garantizar que los datos y la información son precisos, completos, fiables, y que no se modifican ni manipulan de ninguna manera.

- Disponibilidad: Garantizar que los datos y la información estén disponibles para los usuarios autorizados cuando los necesiten, y que no estén sujetos a tiempos de inactividad o interrupciones.

- Privacidad: Identificar y garantizar el cumplimiento de los requisitos relacionados con la información de identificación personal de todas las partes interesadas de la organización, de acuerdo con las leyes y/o regulaciones contractuales.

- Rendición de cuentas: Garantizar que las personas son responsables y rinden cuentas de sus acciones en relación con la seguridad de la información, y que se toman las medidas adecuadas en caso de incumplimiento.

- Cumplimiento: Garantizar que la organización cumple las leyes, reglamentos y normas aplicables relacionados con la seguridad de la información, como TP Global, SOC 1, SOC 2, GDPR, HIPAA, PCI DSS, ISO 27701 e ISO 27001.

- Gestión de riesgos: Garantizar que la organización identifique, evalúe y gestione los riesgos de seguridad de la información, que se establezcan controles y medidas adecuadas para mitigar estos riesgos.

- Continuidad: Garantizar que la organización pueda seguir funcionando y prestando servicios en caso de que se produzca un incidente disruptivo, como riesgos medioambientales, políticos, pérdida de servicios públicos, cortes relacionados con la tecnología y ciberataques.

- Concienciación: Garantizar que todos los empleados y partes interesadas conozcan las políticas y procedimientos de seguridad de la información de la organización y reciban formación sobre cómo identificar y responder a las amenazas e incidentes de seguridad.

7. OBJETIVOS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

- Mantener los niveles de seguridad apropiados para los procesos establecidos en la organización e impulsar la mejora continua.

- Mitigar y gestionar los riesgos de seguridad de la información (clientes, colaboradores, proveedores o terceros), a través de controles internos de la organización alineados con estándares internacionales o requisitos regulatorios de Seguridad de la Información y Privacidad.

- Implementar controles de seguridad para la infraestructura tecnológica, las redes y otros servicios de la organización.

- Gestionar los controles de cambios tecnológicos y de infraestructura tecnológica contribuyendo al cumplimiento de los requisitos de seguridad de la información de la organización. *Cumplimiento de controles de TP Policy.

- Llevar a cabo el proceso de Análisis de Impacto en el Negocio (BIA) para identificar los requisitos de los procesos críticos del negocio que debe abordar el Plan de Continuidad del Negocio.

- Ejecutar planes de continuidad de Negocio para compartir con las partes interesadas.

- Gestionar Pruebas trimestrales sobre los Planes de Continuidad de Negocio.

8. CONTENIDO DE LA POLÍTICA

8.1. Controles organizacionales

8.1.1. Políticas de seguridad de la información.

8.1.1.1. Seguridad de la Información cuenta con un conjunto de políticas aprobadas por la dirección. Estas serán puestas a la disposición de empleados y entes externos.

8.1.1.2. Las políticas de seguridad de la información son revisadas anualmente o cuando se produzcan cambios significativos para garantizar su relevancia y eficacia.

8.1.1.3. Las políticas de seguridad de la información son aprobadas por la alta dirección, publicadas y comunicadas a todo el personal de la organización, tanto como a las partes interesadas.

8.1.2. Funciones y responsabilidades de seguridad de la información.

8.1.2.1. Se definirán y asignarán todas las responsabilidades en materia de seguridad de la información.

8.1.2.2. Se deben segregar los deberes y responsabilidades en conflicto para reducir las oportunidades de modificación no autorizada, involuntaria y/o el uso indebido de los activos de la organización.

8.1.2.3. Se debe requerir que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida y los procedimientos específicos de la organización.

8.1.2.4. Se deben mantener actualizados y documentados los contactos con las autoridades pertinentes y los grupos de interés especial.

8.1.2.5. La organización debe analizar y recopilar toda la información relacionada con amenazas que puedan afectar la seguridad de la información de la organización.

8.1.2.6. Se debe incluir a seguridad de la información desde el inicio de cada proyecto.

8.1.3. Inventario de información y activos

8.1.3.1. La organización debe desarrollar y mantener un inventario de información y activos e incluyendo los propietarios.

8.1.3.2. Se debe documentar e implementar reglas que permitan el uso aceptable y procedimientos para la manipulación de la información y otros activos.

8.1.3.3. El personal y partes interesadas deben según corresponda, devolver todos los activos de la organización que estén bajo su custodia en caso de terminación o cambio de empleo, contrato o acuerdo.

8.1.4. Clasificación de la información de la organización.

8.1.4.1. Se debe clasificar la información de acuerdo con las necesidades de seguridad de la información de la organización con la finalidad de la confidencialidad, integridad, disponibilidad y los requisitos relevantes de las partes interesadas.

8.1.4.2. La organización debe implementar y ejecutar procedimientos para el etiquetado de la información de acuerdo con la estructura acogida por TP.

8.1.4.3. Se deben desarrollar lineamientos, procesos o acuerdos de transferencia de información dentro de la organización y entre otras partes interesadas.

8.1.5. Control de accesos.

8.1.5.1. TP debe establecer procesos y lineamientos para el control del acceso físico y lógico a la información y otros activos asociados a la seguridad de la información basados en los requisitos de seguridad y del negocio.

8.1.5.2. Se debe gestionar el ciclo de vida en su totalidad de las identidades.

8.1.5.3. Los derechos de acceso a la información y activos asociados se deben adecuar, revisar, modificar y eliminar de acuerdo con la política especifica de la organización y lineamientos para el control de acceso.

8.1.6. Seguridad de la información en las relaciones con los proveedores.

8.1.6.1. Para abordar la seguridad de la información en la relación con los proveedores se debe definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información relacionados con proveedores de servicios.

8.1.6.2. TP debe establecer y acordar los requisitos de seguridad de la información con todos los proveedores en función del tipo de relación con el proveedor.

8.1.6.3. Se debe definir e implementar procesos y procedimientos para la gestión de los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.

8.1.6.4. Los proveedores se deben monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información en la prestación de servicios a la organización.

8.1.7. Seguridad de la información para el uso de los servicios en la nube.

8.1.7.1. La organización debe establecer procesos de adquisición, uso, gestión y salida de servicios en la nube, establecidos de acuerdo con los requisitos de seguridad de la información.

8.1.8. Planificación y preparación de la gestión de incidentes de seguridad de la información.

8.1.8.1. Se debe planificar, preparar y gestionar los incidentes de seguridad de la información, definiendo, estableciendo y comunicando procesos, roles y responsabilidades frente a la gestión de incidentes.

8.1.8.2. La organización debe evaluar los eventos de seguridad de la información, y decidir si estos se deben clasificar como incidentes de seguridad de la información.

8.1.8.3. Para la respuesta de incidentes de seguridad de la información la organización debe responder de acuerdo con las políticas y procedimientos documentados.

8.1.8.4. Se debe adquirir conocimiento a partir de los incidentes de seguridad de la información, y usar este para fortalecer y mejorar continuamente los controles relacionados.

8.1.8.5. Se deben establecer, implementar políticas y procedimientos para la identificación, recopilación, adquisición y preservación de la evidencia relevante con eventos de seguridad de la información.

8.1.9. Seguridad de la información durante la interrupción.

8.1.9.1. TP debe planificar como sostener la seguridad de la información en el nivel apropiado durante la interrupción.

8.1.10. Preparación de las TIC para la continuidad del negocio.

8.1.10.1. La preparación de las TIC, la organización debe contar con una planificación, implementación, mantenimiento y pruebas con la capacidad de los objetivos y requisitos de continuidad del negocio y de las TIC.

8.1.11. Requisitos legales, reglamentarios, estatutarios y contractuales.

8.1.11.1. La organización debe identificar, documentar y mantener actualizados los requisitos legales, estatutarios, regulatorios y contractuales.

8.1.12. Derechos de propiedad intelectual.

8.1.12.1. Se debe implementar procedimientos que protejan los derechos de propiedad intelectual.

8.1.13. Protección de registros.

8.1.13.1. Se deben proteger los registros de la organización contra pérdida, destrucción, falsificación, acceso y divulgación no autorizada.

8.1.14. Privacidad y protección de la información de identificación de personal PII.

8.1.14.1. Se debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la información de identificación personal, de acuerdo con las leyes, regulaciones y requisitos contractuales.

8.1.15. Revisión independiente de la seguridad de la información.

8.1.15.1. La organización debe revisar de manera independiente la seguridad de la información, en donde se incluyan los todos los aspectos relevantes tales como: personas, información documentada, procesos y tecnologías. Esta revisión de deberá realizar al menos una vez al año o cuando surjan cambios significativos.

8.1.16. Cumplimiento de políticas, reglas y estándares de seguridad de la información.

8.1.16.1. La organización debe realizar revisiones anuales sobre el cumplimiento de la política de seguridad de la información, lineamientos y estándares.

8.1.16.2. Se deben realizar revisiones anuales sobre seguridad de la información y su implementación en la organización, para garantizar el cumplimiento de los controles, políticas, procedimientos y objetivos.

8.1.16.3. Los procedimientos operativos de las instalaciones donde se procesa la información deben documentarse y ponerse a disposición del personal que lo requiera.

8.2. Controles de Recursos Humanos.

8.2.1. Verificaciones y condiciones del empleo.

8.2.1.1. Se deben llevar a cabo las verificaciones de los antecedentes de todos los candidatos antes de hacer parte de la organización teniendo en cuenta las leyes, regulaciones y éticas aplicables, y que sean proporcionales a los requisitos del negocio.

8.2.1.2. En los acuerdos contractuales de trabajo se deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.

8.2.2. Concientización sobre seguridad de la información.

8.2.2.1. Las personas de la organización y partes interesadas relevantes deben recibir capacitación y formación adecuada, sobre la seguridad de la información y las actualizaciones periódicas de las políticas y procedimientos específicos de seguridad de la información, de acuerdo con su función dentro de la organización.

8.2.3. Proceso disciplinario.

8.2.3.1. La organización debe formalizar y comunicar un proceso disciplinario, para tomar las acciones pertinentes sobre el personal y otras partes interesadas relevantes, que hayan cometido algún tipo de violación a la política de seguridad de la información.

8.2.4. Responsabilidades tras cancelación o cambio de empleo.

8.2.4.1. La organización debe implementar responsabilidades y deberes con lo relacionado a seguridad de la información, para que sigan siendo válidos después de la terminación o cambio del empleo las cuales se definirán, aplicaran y comunicaran a todo el personal y otras partes interesadas.

8.2.4.2. Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información, deben ser identificados, documentados, revisados periódicamente, y firmados por el personal y otras partes interesadas relevantes.

8.2.5. Trabajo Remoto.

8.2.5.1. La organización debe implementar medidas de seguridad cuándo el personal este trabajando de manera remota para proteger la información, a la cual tengan acceso, procesen o almacenen fuera de las instalaciones de la organización.

8.2.6. Informes de eventos de seguridad de la información.

8.2.6.1. La organización debe proporcionar un mecanismo para que el personal comunique eventos de seguridad de la información observados o sospechosos de manera oportuna, a través de canales de comunicación implementados en la organización.

8.3. Controles físicos.

8.3.1.1. Los perímetros de seguridad física se definirán y utilizarán para proteger áreas que contengan información y otros activos asociados.

8.3.1.2. Se debe implementar controles en las entradas y puntos de accesos que protejan las áreas seguras de la organización.

8.3.1.3. La organización debe diseñar e implementar seguridad física para las oficinas, salas e instalaciones.

8.3.1.4. La organización debe implementar controles de monitoreo que detecten continuamente los accesos físicos no autorizados.

8.3.1.5. Para la protección contra amenazas físicas y ambientales, se deben implementar estrategias que permitan proteger a la organización, ante desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

8.3.1.6. Se debe asegurar áreas seguras para el desarrollo de las actividades del negocio y de la organización.

8.3.1.7. La organización debe definir y hacer cumplir los lineamientos estipulados para escritorios limpios, medios de almacenamiento extraíbles y demás implementos que representen un riesgo para las áreas de procesamiento de información.

8.3.1.8. La organización debe definir la ubicación de los equipos de forma segura y protegida.

8.3.1.9. La organización debe proteger a los activos que se encuentren ubicados fuera de las instalaciones.

8.3.1.10. Se deben gestionar los medios de almacenamiento a lo largo del ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de la clasificación y los requisitos de manipulación de la organización.

8.3.1.11. Las instalaciones de procesamiento de la organización deben ser protegidas contra fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

8.3.1.12. El cableado que transporte energía, datos o servicios de información deben ser protegidos contra interceptaciones, interferencias o daños.

8.3.1.13. La organización debe garantizar el mantenimiento de equipos con el fin de asegurar la disponibilidad, integridad y confidencialidad de la información.

8.3.1.14. Los equipos que contengan medios de almacenamiento, datos confidenciales y software con licencia, deben ser borrados de una forma segura antes de la destrucción o reutilización del equipo.

8.4. Controles tecnológicos.

8.4.1.1. **L**a información de la organización almacenada debe ser procesada o accesible a través de dispositivos terminales de usuario protegida.

8.4.1.2. La asignación de los derechos de accesos privilegiados debe ser gestionados y restringidos.

8.4.1.3. La organización debe controlar los accesos a la información y otros activos asociados, de acuerdo con la política de gestión de accesos.

8.4.1.4. El acceso de lectura y escritura al código de fuente, herramientas, aplicaciones de desarrollo y biblioteca de software debe ser gestionada correcta y adecuadamente.

8.4.1.5. La organización debe implementar tecnologías y procedimientos de autenticación segura, con base en los accesos restringidos a la información y la política establecida sobre el control de accesos.

8.4.1.6. Se debe gestionar la capacidad de los recursos los cuales serán supervisados y se ajustarán en consonancia con los requisitos de capacidad actuales y previstos.

8.4.1.7. La protección contra el malware se debe implementar y respaldar por medio de una adecuada concienciación de los usuarios.

8.4.1.8. La organización debe obtener información frente a las vulnerabilidades técnicas de los sistemas de información que se encuentren en uso, y se debe evaluar la exposición de la organización a dichas vulnerabilidades para tomar las acciones apropiadas.

8.4.1.9. Se debe establecer la gestión de configuración la cual se documentará implementará, monitoreará las configuraciones, incluidas las de seguridad de hardware, software, servicios y redes.

8.4.1.10. La información de la organización que se encuentre almacenadas en sistemas, dispositivos o cualquier medio de almacenamiento debe ser eliminada cuándo ya no sea necesaria.

8.4.1.11. La organización debe aplicar el enmascaramiento de los datos los cuales se utilizarán de acuerdo con la política establecida por la organización sobre los controles de acceso, políticas relacionadas, requisitos comerciales y la legislación local.

8.4.1.12. La organización debe aplicar medidas preventivas contra la fuga de datos de los sistemas, redes y cualquier otro dispositivo que procese, almacene o trasmita información sensible.

8.4.1.13. Las copias de seguridad de la información de software y los sistemas deben mantenerse y probarse periódicamente, de acuerdo con la política establecida y acordada sobre las copias de seguridad de la información.

8.4.1.14. Las instalaciones de procesamiento de información de la organización deben contar con suficiente redundancia para cumplir con los requisitos de disponibilidad.

8.4.1.15. Los registros se deben generar, almacenar, proteger y analizar inicios de sesión, actividades, excepciones, fallas y otros eventos relevantes.

8.4.1.16. La organización debe monitorear las redes, sistemas y aplicaciones para la detección de comportamientos anormales, e implementar las acciones pertinentes para evaluar posibles incidentes de seguridad de la información.

8.4.1.17. Los relojes de los sistemas de procesamiento de información que son utilizados por la organización deben estar sincronizados con las fuentes horarias aprobadas.

8.4.1.18. La organización debe restringir y controlar estrictamente, el uso de los programas de utilidad privilegiados que puedan anular los controles de los sistemas y aplicaciones.

8.4.1.19. Se deben implementar procedimientos y controles para gestionar de forma segura la instalación de software en los sistemas operativos.

8.4.1.20. La seguridad de las redes y dispositivos se deben proteger, gestionar y controlar para resguardar la información en los sistemas y aplicaciones.

8.4.1.21. La organización debe identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de los servicios de red.

8.4.1.22. Los grupos de servicios de información, usuarios y sistemas de información se deben segregar en las de redes de la organización.

8.4.1.23. Los accesos a los sitios web externos de la organización deben ser filtrados y gestionados para la reducción a la exposición de contenidos maliciosos.

8.4.1.24. La organización debe definir e implementar reglas para el uso eficaz de la criptografía, incluida la gestión de las claves criptográficas.

8.4.1.25. Se debe establecer y aplicar lineamientos y reglas para el ciclo de vida del desarrollo seguro de software y sistemas.

8.4.1.26. Los requisitos de seguridad de la aplicación se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones.

8.4.1.27. La organización debe establecer, documentar, mantener y aplicar principios de ingeniería de sistemas seguros a cualquier actividad de desarrollo de sistema de información.

8.4.1.28. Se debe aplicar los principios de codificación segura al desarrollo de software.

8.4.1.29. Los procesos de pruebas de seguridad en desarrollo y aceptación se deben definir implementar en el ciclo de vida del desarrollo.

8.4.1.30. La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo subcontratado.

8.4.1.31. La separación de los entornos de desarrollo, pruebas y producción deben estar separados y asegurados.

8.4.1.32. Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios de la organización.

8.4.1.33. La organización debe proteger, y gestionar adecuadamente la información de las pruebas.

8.4.1.34. La organización debe planificar y acordar entre el evaluador y la dirección, la protección de los sistemas de información durante las pruebas de auditoría, y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos.

9. CONTROL DE CAMBIOS Y CICLO DE APROBACIÓN.

FECHA	VERSIÓN	DESCRIPCIÓN	CICLO DE APROBACIÓN
08/05/2012	1	Primera versión de la definición de política y objetivos del SGSI.	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Carlos Carrizosa
19/03/2014	2	Revisión de política y objetivos del SGSI 2013/2014	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
07/04/2015	3	Revisión y actualización del documento	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
09/02/2016	4	Revisión y actualización del documento	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
14/08/2017	5	Revisión y actualización del documento	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
30/08/2018	6	Revisión y actualización del documento (logo)	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
29/04/2019	7	Ampliación del alcance de la política e integración con los Sistemas de gestión.	**Elabora:** Gustavo Olaya- Yesenia Brand **Revisa:** Ivan Diaz- Ana Gomez **Aprueba:** Carlos Carrizosa- Omar Ladino
28/10/2020	8	Revisión y correcciones menores al texto	**Elabora:** Luis Gonzalez – William Ricaurte **Revisa:** Alvaro Guerrero **Aprueba:** Carlos Carrizosa
13/09/2021	9	Revisión y correcciones menores al texto	**Elabora:** Luis Gonzalez **Revisa:** Alvaro Guerrero **Aprueba:** Carlos Carrizosa
27/09/2022	10	Ampliación y mejora del contenido de la política.	**Elabora:** Jose Montañez **Revisa:** Luis Gonzalez **Aprueba:** Claudio Esteves
01/02/2023	11	Se amplía el alcance en lo relacionado a teletrabajo.	**Elabora:** Jose Montañez **Revisa:** Luis Gonzalez **Aprueba:** Claudio Esteves

24/03/2023	12	Ampliación y mejora del contenido de la política.	**Elabora:** Luis Gonzalez-Liliana Villar **Revisa:** Javier Fernandez **Aprueba:** Claudio Esteves
21/08/2024	13	Actualización de política de acuerdo con los controles de la versión ISO 27001:2022.	**Elabora:** Liliana Villar **Revisa:** Javier Fernandez **Aprueba:** Claudio Esteves
18/11/2024	13	Revisión sin cambios, ajustes menores en el documento.	**labora:** Liliana Villar **Revisa:** Javier Fernández **Aprueba:** Claudio Esteves
01/04/2025	14	Actualización de logo y portada de la política.	**labora:** Estefania Castañeda **Revisa:** Javier Fernández **Aprueba:** Claudio Esteves